ManageEngine
Identity Access

Smarter security at every sign-in

Decide who gets in—to every laptop, every app, every time.



One login. Everything unlocked.

For most workforces, access is decided once, at the first sign-in. The desktop, every application, and the network all inherit that decision. So does anyone holding a stolen password.

The applications are protected. The laptop isn't.

Most organizations put MFA on their applications and left the first sign-in of the day, the device, on a password.



MFA that ends at the browser

Application-level MFA covers what a user opens in a browser tab. It doesn't cover the sign-in that unlocks the machine underneath—the one that grants the local session every application then inherits.



Codes that can be handed over

Most workforce MFA still runs on one-time codes, sent by SMS or email or generated in an app. A user can be talked into reading one aloud or typing it into a fake sign-in page. A code is a short-lived shared secret, not a phishing-resistant credential.



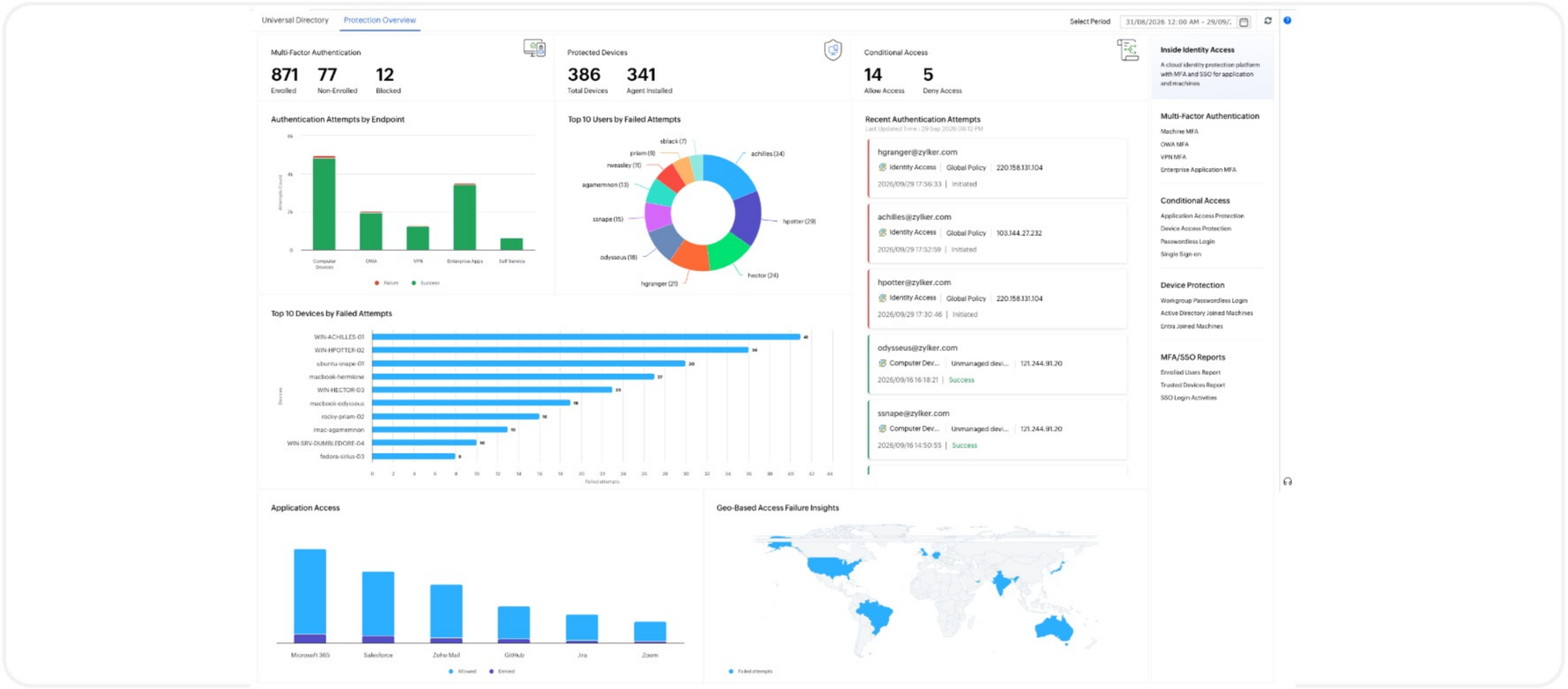
Machines the directory never reached

Remote hires, contractor machines, and devices bought outside IT's process often never join a domain. The only thing between the user and the desktop is a local account and a password, and no central sign-in policy reaches it.

FIDO Alliance, State of Passkeys 2026—57% of organizations that have deployed passkeys still use a phishable method for primary day-to-day sign-in.

One console to decide who gets in

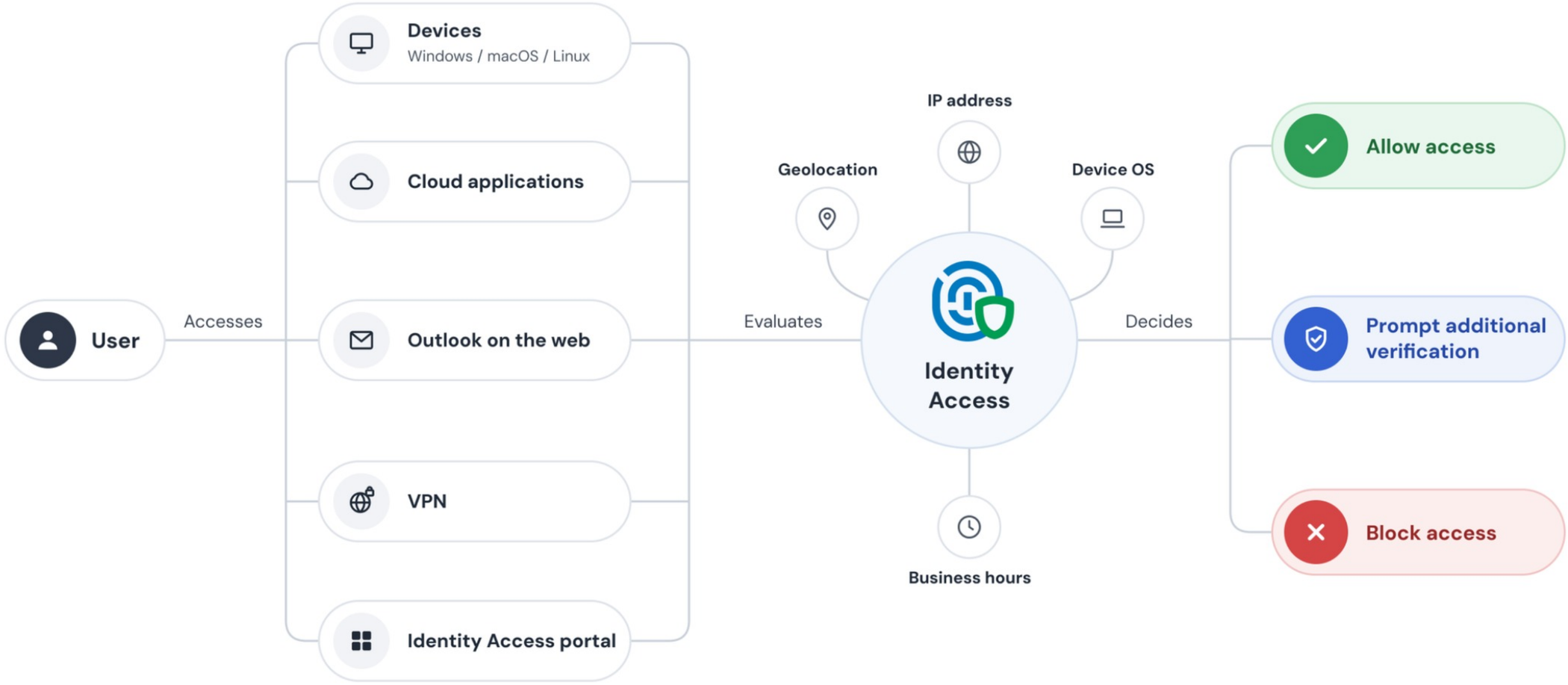
ManageEngine Identity Access sits in front of everything your people sign in to: their laptops, cloud applications, VPN, and Outlook on the web. Each sign-in is checked for who is asking, from where, and on what device, then allowed, denied, or challenged for more.



Where you run Active Directory, Identity Access imports your users from it. Where you don't, it doesn't need one.

Every sign-in, judged in context

Five entry points, four signals, three outcomes.



Secured from the very first login

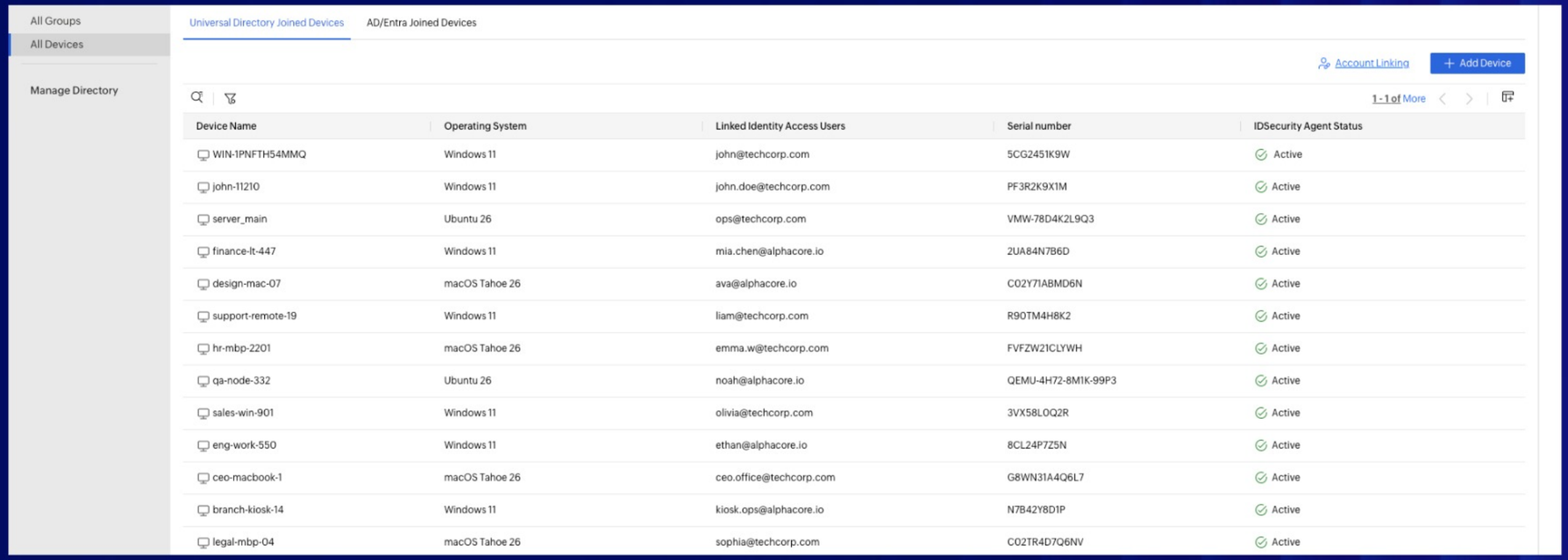
Secure sign-in for laptops outside the domain

Enroll Windows, macOS, and Linux machines directly into Identity Access, with no Active Directory, or on-premises server required. Users sign in to the device with their Identity Access account, and MFA protects that sign-in.

Password sign-in that can't be phished

FIDO2 passkeys and smart cards—PIV and CAC—replace the password at device login, cloud applications, the portal, and VPN. No shared secret exists for an attacker to capture, replay, or ask a user to hand over.

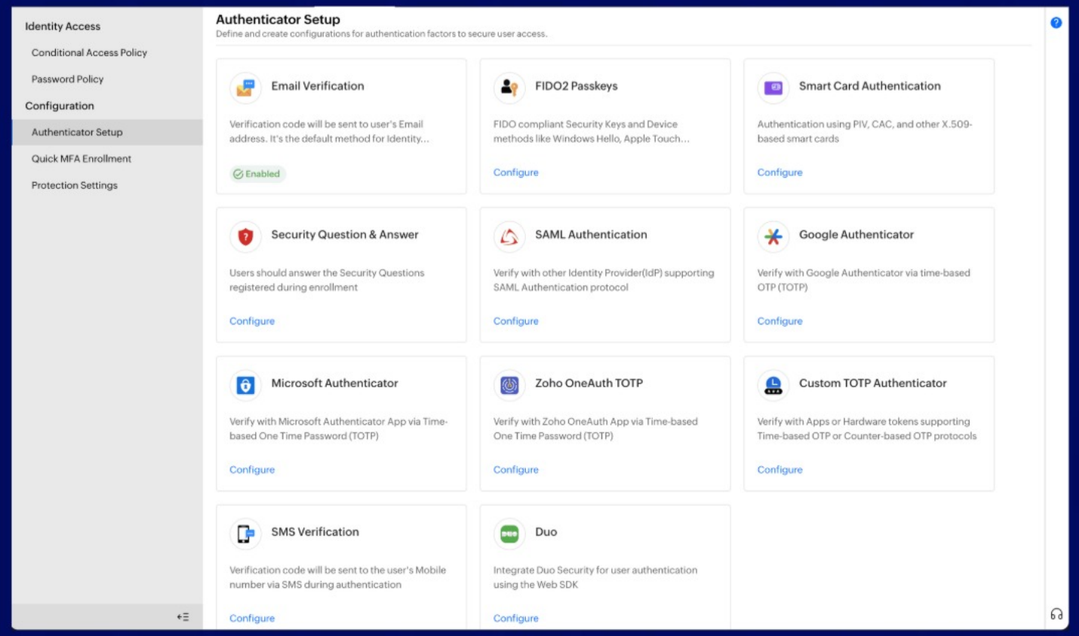
FIDO2 and PIV/CAC are the authenticator types CISA identifies as phishing-resistant.



Device Name	Operating System	Linked Identity Access Users	Serial number	IDSecurity Agent Status
WIN-1PNFTH54MMQ	Windows 11	john@techcorp.com	5CG2451K9W	Active
john-11210	Windows 11	john.doe@techcorp.com	PF3R2K9X1M	Active
server_main	Ubuntu 26	ops@techcorp.com	VMW-78D4K2L9Q3	Active
finance-lt-447	Windows 11	mia.chen@alphacore.io	2UA84N7B6D	Active
design-mac-07	macOS Tahoe 26	ava@alphacore.io	C02Y71ABMD6N	Active
support-remote-19	Windows 11	liam@techcorp.com	R90TM4H8K2	Active
hr-mbp-2201	macOS Tahoe 26	emma.w@techcorp.com	FVFZW21CLYWH	Active
qa-node-332	Ubuntu 26	noah@alphacore.io	QEMU-4H72-8M1K-99P3	Active
sales-win-901	Windows 11	olivia@techcorp.com	3VX58LOQ2R	Active
eng-work-550	Windows 11	ethan@alphacore.io	8CL24P7Z5N	Active
ceo-macbook-1	macOS Tahoe 26	ceo.office@techcorp.com	G8WN31A4Q6L7	Active
branch-kiosk-14	Windows 11	kiosk.ops@alphacore.io	N7B42Y8D1P	Active
legal-mbp-04	macOS Tahoe 26	sophia@techcorp.com	C02TR4D7Q6NV	Active

Your factors, everywhere you sign in

The strongest factors can be reserved for the applications that warrant them.



Phishing-resistant

FIDO2 passkeys (security keys, Windows Hello, Touch ID) and smart cards (PIV, CAC, and other X.509 certificates).

Everything you already have

Authenticator apps and TOTP or HOTP tokens, SAML 2.0 identity providers, Duo, email and SMS codes, and security questions.

Every sign-in on the machine

Windows, macOS, and Linux login, plus UAC prompts, RDP, SSH, and sudo/su, online or offline.

Network and on-premises endpoints

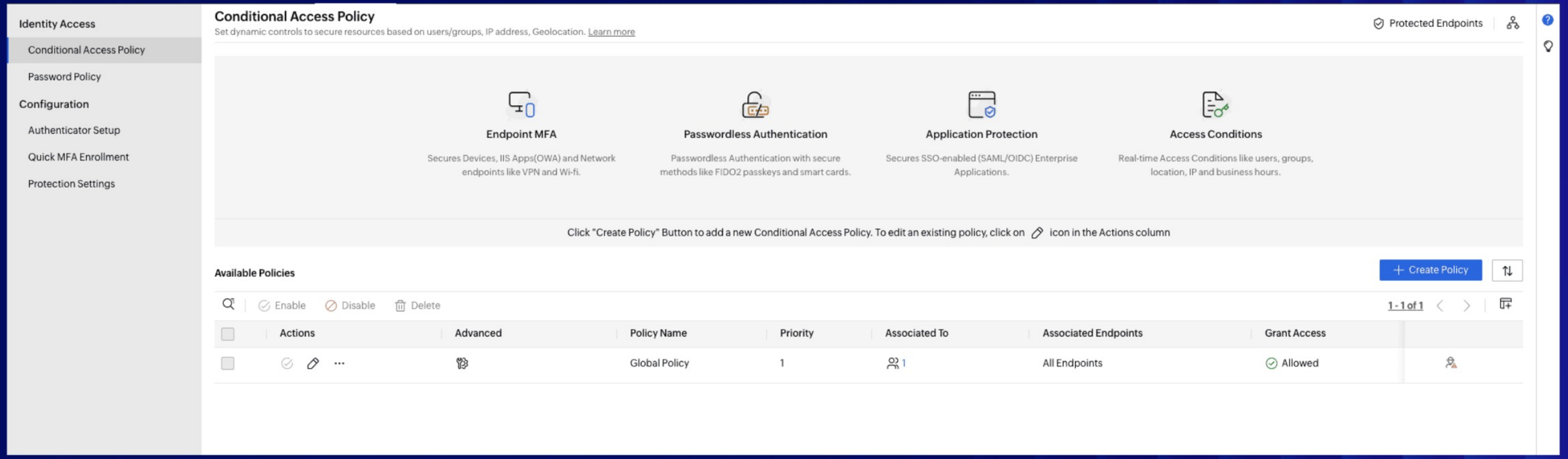
VPN and RADIUS-based access, Outlook on the web, and IIS-hosted applications.

Custom applications

Any SAML or OIDC application outside the preintegrated catalog, each with its own MFA requirement.

Same user, different answer

Every access attempt is evaluated against IP address, geolocation, business hours, and device OS. The policy allows, denies, or requires an additional factor—so one credential doesn't behave the same way from everywhere.



The policy allows, denies, or requires an additional factor — so one credential doesn't behave the same way from everywhere.

ManageEngine

How strict, how often, for whom

Advanced settings tune MFA separately for the portal and applications, Windows machines, and VPN.



Time-bound prompts

Users must finish MFA within a set window, configured separately for app, machine, and VPN sign-ins.



Trusted devices

Skip repeat prompts on a trusted browser or machine for set hours or days. New browsers still get challenged.



Enrollment first

Block users missing a required factor, or make them finish enrolling before they get in.



Brakes on guessing

Show a CAPTCHA on MFA prompts, on every attempt or after a set number of failures.

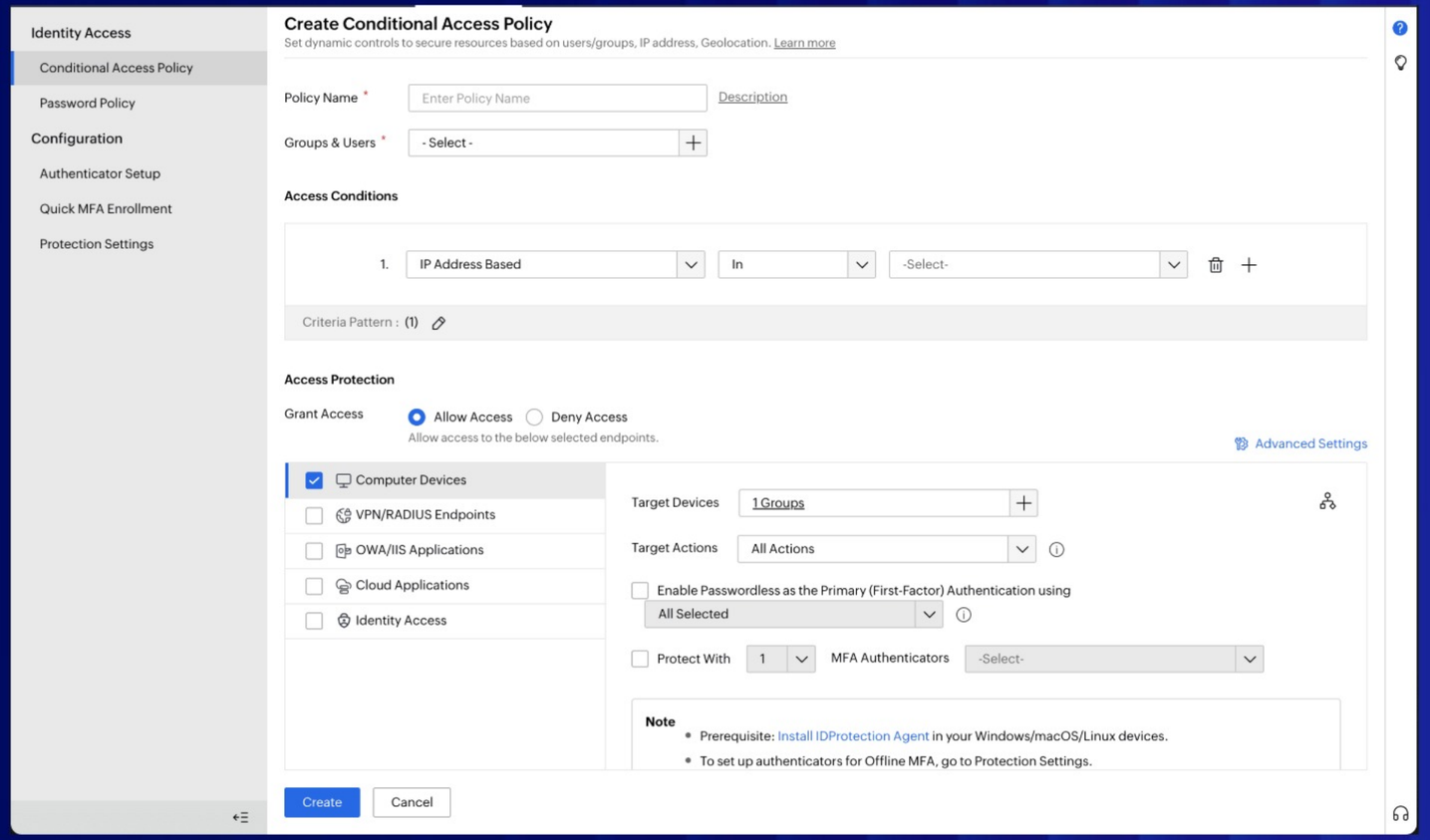
Friction where it’s warranted

Per-app MFA

Apply different MFA requirements to different applications. The same user can sail into a wiki and face a passkey prompt at the finance system.

Step-up verification

Inside the portal, disruptive actions—deleting users, groups, or directories, or bulk-disenrolling users—require a fresh verification before they execute.



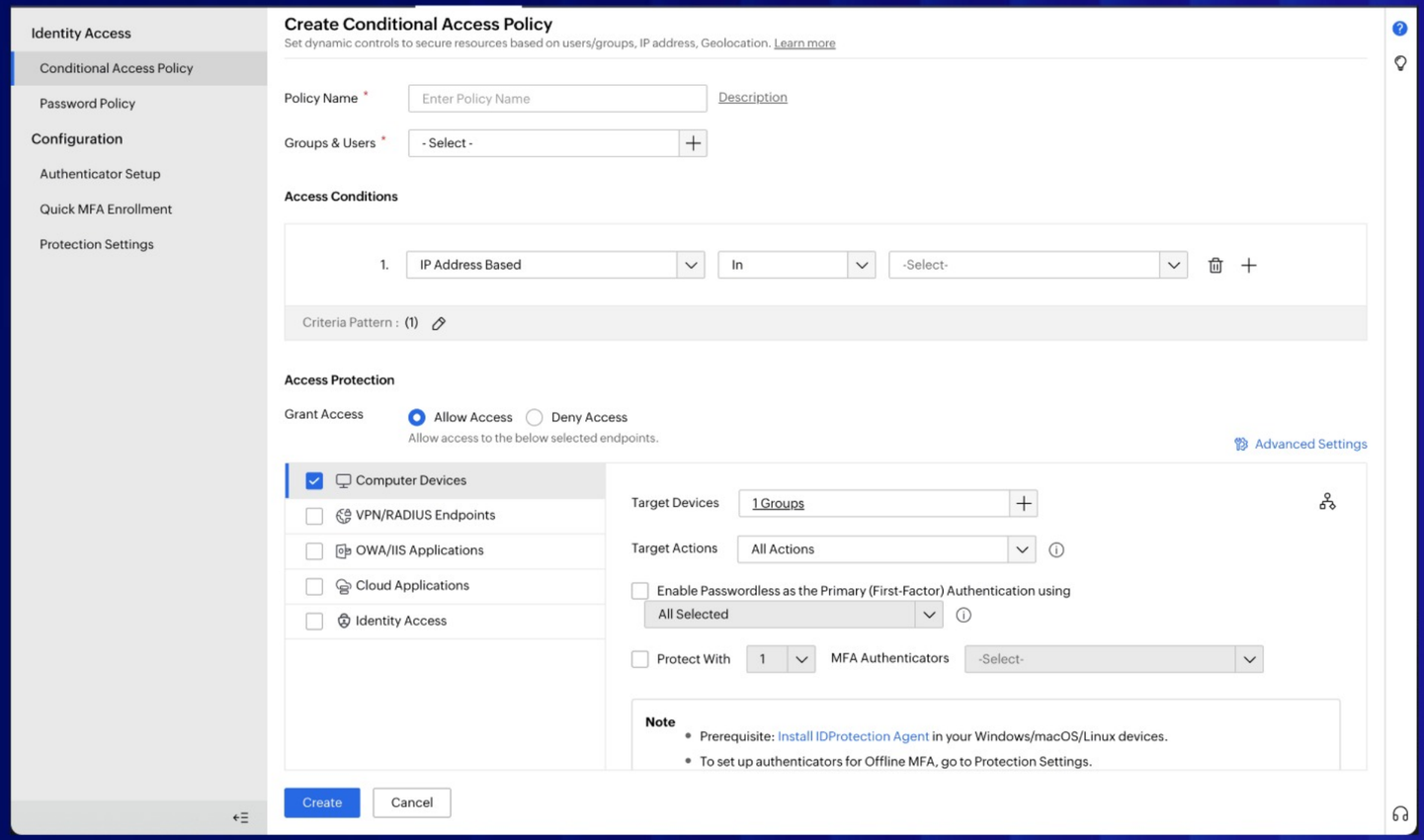
Built to keep working

MFA that works offline

When a laptop can't reach Identity Access, the IDSecurity Agent still challenges the user against locally cached credentials, so dropping offline is neither a lockout nor a way around MFA. If a user's enrolled device is unavailable, a short-lived, one-time emergency code can be issued.

One sign-in, every application

Over 500 applications are pre-integrated and ready to configure—and anything outside that list can be added as a custom application. Assign users per application, and pair each one with its own MFA requirement.



ManageEngine

Where Identity Access fits

Identity Access usually earns its place for one of three reasons:



No directory at all

Cloud-native teams running on laptops with local accounts, no server to maintain and no domain to join.



Active Directory, but not only Windows

Organizations with AD in place and a growing share of macOS and Linux machines it was never built to reach.



Already issuing smart cards

Environments with PIV or CAC deployments that need those cards to work as a primary credential, not a side option.

Evaluate it in your own environment

Bring your mix of Windows, Mac, and Linux, your directory or absence of one, and the applications your people actually use.

Request a demo

ManageEngine
Identity Access

Thank you